nytimes.com

N.S.A. Able to Foil Basic Safeguards of Privacy on Web

Nicole Perlroth, Jeff Larson, Scott Shane

17-21 minutes

- Sept. 5, 2013

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named

Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor.

Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own “back door” in all encryption, it set out to accomplish the same goal by stealth.

The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated.

The N.S.A. hacked into target computers to snare messages before they were encrypted. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world’s most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.

“For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies,” said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. “Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable.”

When the British analysts, who often work side by side with N.S.A. officers, were first told about the program, another memo said, “those not already briefed were gobsmacked!”

An intelligence budget document makes clear that the effort is still going strong. “We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet traffic,” the director of national intelligence, James R. Clapper Jr., wrote in his budget request for the current year.

In recent months, the documents disclosed by Mr. Snowden have described the N.S.A.’s reach in scooping up vast amounts of communications around the world. The encryption documents now show, in striking detail, how the agency works to ensure that it is actually able to read the information it collects.

The agency’s success in defeating many of the privacy protections offered by encryption does not change the rules that prohibit the deliberate targeting of Americans’ e-mails or phone calls without a warrant. But it shows that the agency, which was sharply rebuked by a federal judge in 2011 for violating the rules and misleading the Foreign Intelligence Surveillance Court, cannot necessarily be restrained by privacy technology. N.S.A. rules permit the agency to store any encrypted communication, domestic or foreign, for as long as the agency is trying to decrypt it or analyze its technical features.

The N.S.A., which has specialized in code-breaking since its creation in 1952, sees that task as essential to its mission. If it cannot decipher the messages of terrorists, foreign spies and other adversaries, the United States will be at serious risk, agency officials say.

Just in recent weeks, the Obama administration has called on the intelligence agencies for details of communications by leaders of Al Qaeda about a terrorist plot and of Syrian officials' messages about the chemical weapons attack outside Damascus. If such communications can be hidden by unbreakable encryption, N.S.A. officials say, the agency cannot do its work.

But some experts say the N.S.A.'s campaign to bypass and weaken communications security may have serious unintended consequences. They say the agency is working at cross-purposes with its other major mission, apart from eavesdropping: ensuring the security of American communications.

Some of the agency's most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer, or SSL; virtual private networks, or VPNs; and the protection used on fourth-generation, or 4G, smartphones. Many Americans, often without realizing it, rely on such protection every time they send an e-mail, buy something online, consult with colleagues via their company's computer network, or use a phone or a tablet on a 4G network.

For at least three years, one document says, GCHQ, almost certainly in collaboration with the N.S.A., has been looking for ways into protected traffic of popular Internet companies: Google, Yahoo, Facebook and Microsoft's Hotmail. By 2012, GCHQ had developed "new access opportunities" into Google's systems, according to the document. (Google denied giving any government access and said it had no evidence its systems had been breached).

"The risk is that when you build a back door into systems, you're

not the only one to exploit it," said Matthew D. Green, a cryptography researcher at Johns Hopkins University. "Those back doors could work against U.S. communications, too."

Image

Credit...Associated Press

Paul Kocher, a leading cryptographer who helped design the SSL protocol, recalled how the N.S.A. lost the heated national debate in the 1990s about inserting into all encryption a government back door called the Clipper Chip.

“And they went and did it anyway, without telling anyone,” Mr. Kocher said. He said he understood the agency’s mission but was concerned about the danger of allowing it unbridled access to private information.

“The intelligence community has worried about ‘going dark’ forever, but today they are conducting instant, total invasion of privacy with limited effort,” he said. “This is the golden age of spying.”

A Vital Capability

The documents are among more than 50,000 shared by The Guardian with The New York Times and ProPublica, the nonprofit news organization. They focus on GCHQ but include thousands from or about the N.S.A.

Intelligence officials asked The Times and ProPublica not to publish this article, saying it might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read. The news organizations removed some specific facts but decided to publish the article because of the value of a public debate about government actions that weaken the most powerful privacy tools.

The files show that the agency is still stymied by some encryption, as Mr. Snowden suggested in a question-and-answer session on The Guardian’s Web site in June.

“Properly implemented strong crypto systems are one of the few things that you can rely on,” he said, though cautioning that the N.S.A. often bypasses the encryption altogether by targeting the computers at one end or the other and grabbing text before it is encrypted or after it is decrypted.

The documents make clear that the N.S.A. considers its ability to decrypt information a vital capability, one in which it competes with China, Russia and other intelligence powers.

“In the future, superpowers will be made or broken based on the strength of their cryptanalytic programs,” a 2007 document said. “It is the price of admission for the U.S. to maintain unrestricted access to and use of cyberspace.”

The full extent of the N.S.A.’s decoding capabilities is known only to a limited group of top analysts from the so-called Five Eyes: the N.S.A. and its counterparts in Britain, Canada, Australia and New Zealand. Only they are cleared for the Bullrun program, the successor to one called Manassas — both names of an American Civil War battle. A parallel GCHQ counterencryption program is called Edgehill, named for the first battle of the English Civil War of the 17th century.

Unlike some classified information that can be parceled out on a strict “need to know” basis, one document makes clear that with Bullrun, “there will be NO ‘need to know.’ ”

Only a small cadre of trusted contractors were allowed to join Bullrun. It does not appear that Mr. Snowden was among them, but he nonetheless managed to obtain dozens of classified documents referring to the program’s capabilities, methods and sources.

Ties to Internet Companies

When the N.S.A. was founded, encryption was an obscure technology used mainly by diplomats and military officers. Over the last 20 years, it has become ubiquitous. Even novices can tell that their exchanges are being automatically encrypted when a tiny padlock appears next to a Web address.

Because strong encryption can be so effective, classified N.S.A. documents make clear, the agency's success depends on working with Internet companies — by getting their voluntary collaboration, forcing their cooperation with court orders or surreptitiously stealing their encryption keys or altering their software or hardware.

According to an intelligence budget document leaked by Mr. Snowden, the N.S.A. spends more than $250 million a year on its Sigint Enabling Project, which "actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" to make them "exploitable." Sigint is the acronym for signals intelligence, the technical term for electronic eavesdropping.

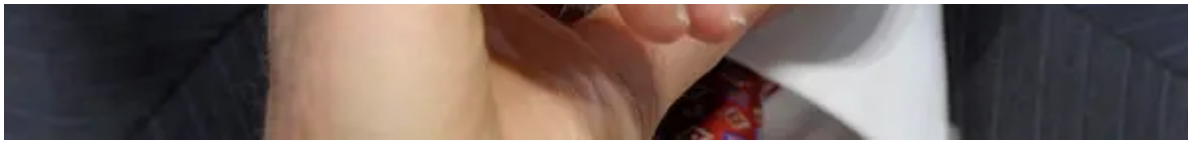
By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors or by exploiting security flaws, according to the documents. The agency also expected to gain full unencrypted access to an unnamed major Internet phone call and text service; to a Middle Eastern Internet service; and to the communications of three foreign governments.

In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the

American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times.

The 2013 N.S.A. budget request highlights “partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses” — that is, to allow more eavesdropping.

At Microsoft, as The Guardian has reported, the N.S.A. worked with company officials to get pre-encryption access to Microsoft’s most popular services, including Outlook e-mail, Skype Internet phone calls and chats, and SkyDrive, the company’s cloud storage service.



Image

Credit...Susan Walsh/Associated Press

Microsoft asserted that it had merely complied with “lawful demands” of the government, and in some cases, the collaboration was clearly coerced. Some companies have been asked to hand the government the encryption keys to all customer communications, according to people familiar with the

government's requests.

N.S.A. documents show that the agency maintains an internal database of encryption keys for specific commercial products, called a Key Provisioning Service, which can automatically decode many messages. If the necessary key is not in the collection, a request goes to the separate Key Recovery Service, which tries to obtain it.

How keys are acquired is shrouded in secrecy, but independent cryptographers say many are probably collected by hacking into companies' computer servers, where they are stored. To keep such methods secret, the N.S.A. shares decrypted messages with other agencies only if the keys could have been acquired through legal means. "Approval to release to non-Sigint agencies," a GCHQ document says, "will depend on there being a proven non-Sigint method of acquiring keys."

Simultaneously, the N.S.A. has been deliberately weakening the international encryption standards adopted by developers. One goal in the agency's 2013 budget request was to "influence policies, standards and specifications for commercial public key technologies," the most common encryption method.

Cryptographers have long suspected that the agency planted vulnerabilities in a standard adopted in 2006 by the National Institute of Standards and Technology and later by the International Organization for Standardization, which has 163 countries as members.

Classified N.S.A. memos appear to confirm that the fatal weakness, discovered by two Microsoft cryptographers in 2007, was engineered by the agency. The N.S.A. wrote the standard and

aggressively pushed it on the international group, privately calling the effort “a challenge in finesse.”

“Eventually, N.S.A. became the sole editor,” the memo says.

Even agency programs ostensibly intended to guard American communications are sometimes used to weaken protections. The N.S.A.’s Commercial Solutions Center, for instance, invites the makers of encryption technologies to present their products to the agency with the goal of improving American cybersecurity. But a top-secret N.S.A. document suggests that the agency’s hacking division uses that same program to develop and “leverage sensitive, cooperative relationships with specific industry partners” to insert vulnerabilities into Internet security products.

By introducing such back doors, the N.S.A. has surreptitiously accomplished what it had failed to do in the open. Two decades ago, officials grew concerned about the spread of strong encryption software like Pretty Good Privacy, designed by a programmer named Phil Zimmermann. The Clinton administration fought back by proposing the Clipper Chip, which would have effectively neutered digital encryption by ensuring that the N.S.A. always had the key.

That proposal met a backlash from an unlikely coalition that included political opposites like Senator John Ashcroft, the Missouri Republican, and Senator John Kerry, the Massachusetts Democrat, as well as the televangelist Pat Robertson, Silicon Valley executives and the American Civil Liberties Union. All argued that the Clipper would kill not only the Fourth Amendment, but also America’s global technology edge.

By 1996, the White House backed down. But soon the N.S.A.

began trying to anticipate and thwart encryption tools before they became mainstream.

Each novel encryption effort generated anxiety. When Mr. Zimmermann introduced the Zfone, an encrypted phone technology, N.S.A. analysts circulated the announcement in an e-mail titled “This can’t be good.”

But by 2006, an N.S.A. document notes, the agency had broken into communications for three foreign airlines, one travel reservation system, one foreign government’s nuclear department and another’s Internet service by cracking the virtual private networks that protected them.

By 2010, the Edgehill program, the British counterencryption effort, was unscrambling VPN traffic for 30 targets and had set a goal of an additional 300.

But the agencies’ goal was to move away from decrypting targets’ tools one by one and instead decode, in real time, all of the information flying over the world’s fiber optic cables and through its Internet hubs, only afterward searching the decrypted material for valuable intelligence.

A 2010 document calls for “a new approach for opportunistic decryption, rather than targeted.” By that year, a Bullrun briefing document claims that the agency had developed “groundbreaking capabilities” against encrypted Web chats and phone calls. Its successes against Secure Sockets Layer and virtual private networks were gaining momentum.

But the agency was concerned that it could lose the advantage it had worked so long to gain, if the mere “fact of” decryption became widely known. “These capabilities are among the Sigint

community's most fragile, and the inadvertent disclosure of the simple 'fact of' could alert the adversary and result in immediate loss of the capability," a GCHQ document warned.

Since Mr. Snowden's disclosures ignited criticism of overreach and privacy infringements by the N.S.A., American technology companies have faced scrutiny from customers and the public over what some see as too cozy a relationship with the government. In response, some companies have begun to push back against what they describe as government bullying.

Google, Yahoo, Microsoft and Facebook have pressed for permission to reveal more about the government's requests for cooperation. One e-mail encryption company, Lavabit, closed rather than comply with the agency's demands for customer information; another, Silent Circle, ended its e-mail service rather than face such demands.

In effect, facing the N.S.A.'s relentless advance, the companies surrendered.

Ladar Levison, the founder of Lavabit, wrote a public letter to his disappointed customers, offering an ominous warning. "Without Congressional action or a strong judicial precedent," he wrote, "I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States."

Something went wrong. Please try again later.